REMARKS

Claims 1-67 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 102(e) Rejection:

The Office Action rejected claims 1, 4-10, 19, 21-26, 36, 38-42, 48, 52-60, 62, 66 and 67 under 35 U.S.C. § 102(e) as being anticipated by Takahashi et al. (U.S. Publication 2002/0194237) (hereinafter "Takahashi"). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 1, Takahashi fails to disclose *a first arithmetic circuit comprising a first plurality of arithmetic structures feeding back high order bits of a previously executed single arithmetic instruction of a processor instruction set in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures*. In rejecting claim 1, the Examiner cites paragraphs [0009] and [0017] of Takahashi as disclosing these aspects of the claimed invention. As noted in paragraph [0009], Takahashi is directed to a multi-function processor that can perform multiple types of modulo mathematic operations (e.g., modulo multiplication, modulo exponentiation, and modulo reduction).

Paragraph [0017] of Takahashi describes that one or more of such processors can be included in a system for encrypting/decrypting data. This paragraph also describes that each such processor receives operands for a particular modulo mathematic operation, stores the operands in an operand storage portion, performs the particular modulo mathematic operation using the stored operands, and outputs a final result after iteratively computing a running partial product and post-processing the final partial product. Other portions of Takahashi describe that different bits of the originally received and stored operands for the particular modulo mathematic operation are supplied to different

pipeline stages of the processor for computing the running partial product. In other words, Takahashi describes a processor that is configured to perform one modulo mathematic operation at a time, using operands that are explicitly supplied to it for that operation. For example, each of paragraphs [0010] – [0016] describes a different modulo mathematic operation (e.g., a modulo multiplication type operation, such as AB mod N, or a modulo N exponentiation, such as A^E mod N) that can be performed by the multi-function modulo processor of Takahashi. As described in these and other paragraphs in Takahashi, for each of these mathematic operations, all of the operands for the operation are explicitly provided to (received by) the processor for that operation and are used in computing a result. Contrary to the Examiner's assertion, there is nothing in the cited passages, or elsewhere in Takahashi, that describes feeding back high order bits of a previously executed single arithmetic instruction of a processor instruction set that were generated by a first arithmetic circuit, to a second arithmetic circuit. Furthermore, Takahashi does not describe any instructions of the processor's instruction set, much less any type of feedback that occurs between two different instructions (i.e. two instances of any of the instructions of the processor's instruction set) when they are executed.

Further regarding claim 1, Takahashi fails to disclose *the second arithmetic circuit generating a first partial result of a currently executing single arithmetic instruction of the processor instruction set in the public-key cryptography application, wherein the currently executing single arithmetic instruction does not include an explicit source operand for specifying the high order bits, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit*. The Examiner cites paragraphs [0017], [0038], and [0044] of Takahashi as disclosing these aspects of Applicants' invention. The Examiner notes that these paragraphs describe that the pipeline portion of the processor receives operands from the operand storage portion of the processor. Contrary to the Examiner's suggestion, the operands that are stored in the operand storage portion of the processor and that are received by the pipeline portion

of the processor are not high order bits of a previously executed single arithmetic instruction of the processor's instruction set. No such feedback from a previously executed instruction to another (currently executing) instruction is disclosed in Takahashi. Instead, the operands that are stored in the operand storage portion of the processor and that are received by the pipeline portion of the processor are operands that were received by the processor for the currently executing modulo mathematic operation.

The Examiner submits that paragraph [0017] of Takahashi describes, "pipeline storage processing (multiplication, summation) stage iteratively computing a running partial product using one or more received operands a predetermined number of times; post processing stage to receive final partial product and compute result" (emphasis added). Applicants again assert that there is nothing in Takahashi describing that any of the received operands are high order bits fed back from a previously executed single arithmetic instruction. The Examiner submits that paragraph [0044] discloses, "receive bit stored in the current highest order position; first carry-save processor (a0 position); second carry-save processor (a1 position); third carry-save processor (a2);…)" The Examiner's suggestion that this passage describes an arithmetic circuit of Takahashi receiving high order bits fed back from a previously executed single arithmetic instruction are completely unsupported in the reference itself. The cited passage *actually* states, in its entirety (with emphasis added):

> [0044] Each of the carry save processors 422-1, 422-2, 422-3, 422-4 is coupled to receive a single bit of data stored in the first operand register 414, all of the data bits stored in the second operand register 416, and all of the data bits stored in the third operand register 418. Specifically, with respect to the data stored in the first operand register 414, the first carry-save processor 422-1 is coupled to receive the single data bit stored in the least significant bit position of the first operand register (e.g., the a.sub.0 position), the second carry-save adder 422-2 is coupled to receive the single data bit stored in the next position of the first operand register 414 (e.g., the a, position), third carry-save adder 422-3 the next (e.g., the a.sub.2 position), and the fourth carry-save adder 422-4 the next (e.g., the a.sub.3 position). As will become more apparent when a discussion of the iterative calculations performed by the pipeline processing unit 306 is provided, the data stored in the first operand register 414 is shifted to the

> right four bits after each iteration, until all of the data bits stored in the first operand register 414 are utilized in the calculational process.

In other words, this passage describes, in detail, how the individual bits of the operands that were received (and stored) for a single modulo mathematic operation are distributed to different carry-save adders in order to perform the desired calculation. **This teaches absolutely nothing about the above-referenced limitations of Applicants' claim**. For example, nothing in the cited passage, or elsewhere in Takahashi, discloses a (second) arithmetic circuit that generates a first partial result representing the high order bits (i.e. high order bits fed back from a previously executed single arithmetic instruction and not explicitly specified as a source operand for a currently executing instruction) summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit, as in Applicants' claim.

Applicants' claim describes a relationship between a currently executing single arithmetic instruction of the processor instruction set and a previously executed single arithmetic instruction of the processor instruction set. Thus, the claim defines a relationship between the executions of two successive single arithmetic instructions of the processor instruction set. Applicants assert that the Examiner has not identified a single arithmetic instruction of a processor instruction set (i.e. an instruction implemented in a processor) in Takahashi whose execution causes the performance of the specific collection of operations described in Applicants' claim by the circuitry disclosed in Takahashi, or results in the relationships between successive instruction executions (i.e. between the executions of two distinct instances of single arithmetic instructions) recited in the claim.

Takahashi describes operations of a modulo processor architecture that are used to implement a single arithmetic instruction (one of several modulo mathematic operations that can be performed by the processor). Takahashi describes feedback between

operations of the processor that collectively implement this single arithmetic instruction. Takahashi does not describe implicit feedback (or an implicit relationship) between this single arithmetic instruction and a previously executed single arithmetic instruction of the processor's instruction set, as required by Applicants' claim, i.e. adding high order bits of a previously executed single arithmetic instruction without specifying these bits as a source operand of the currently executing single arithmetic instruction. Applicants assert that Takahashi clearly does not disclose these aspects of Applicants' claimed invention.

"[U]nless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN, Inc. v. VeriSign et al.*, Case No. 07-1565 (Fed. Cir., Oct. 20, 2008). Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The identical invention must be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed in detail above, Takahashi clearly does not disclose the single arithmetic processor instruction of Applicants' claim, the recited operations performed by first and second arithmetic circuits during execution of such an instruction, or the recited relationships between successive instruction executions. Therefore, Takahashi does not anticipate claim 1.

For at least the reasons stated above, Applicants assert that the Examiner has failed to establish a *prima facie* rejection of claim 1.

Claims 38 and 66 include limitations that are similar to those of claim 1 discussed above, and the Examiner rejected claims 38 and 66 for the same reasons as claim 1. Therefore, the arguments presented above apply with equal force to these claims, as well.

Claims 21, 53, and 67 include limitations that are similar to those of claim 1 discussed above, and the Examiner rejected claims 38 and 66 for the same reasons as claim 1. Therefore, the arguments presented above apply with equal force to these claims, as well. In addition, these claims include limitations that are not included in claim 1 and which the Examiner did not address in his rejection of these claims. Therefore, the rejection is improper. For example, claim 21 includes the following: <u>*supplying a third number*</u> *to the second arithmetic circuit*; and *the second arithmetic circuit generating a first partial result of a currently executing single arithmetic instruction of the processor instruction set in the public-key cryptography application, wherein the currently executing single arithmetic instruction does not include an explicit source operand for specifying the high order bits, the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number* <u>*and with the third number*</u>*, the summing being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit*. Applicants assert that nothing is Takahashi discloses these limitations of claim 21. Therefore Takahashi does not anticipate claim 21. Claims 53 and 67 include limitations similar to those of claim 21. Therefore, the arguments presented above and directed to claim 21 apply with equal force to these claims, as well.

For at least the reasons stated above, Applicants assert that the Examiner has failed to establish a *prima facie* rejection of claims 21, 38, 53, 66, and 67.

<u>**Section 103(a) Rejections**</u>**:**

The Office Action rejected claims 2, 3, 15-18, 27-29, 35 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Takahashi in view of Lasher et al. (U.S. Patent 4,863,247) (hereinafter "Lasher"), claims 11, 20, 30, 31, 37, 47 and 61 as being unpatentable over Takahashi in view of Stribaek et al. (U.S. Patent 7,181,484) (hereinafter "Stribaek"), and claims 12-14, 32-34, 49-51 and 63-65 as being unpatentable over Takahashi in view of Chen et al. (U.S. Patent 6,687,725) (hereinafter "Chen2").

Applicants respectfully traverse these rejections for at least the reasons given above in regard to the independent claims.

In regard to the rejections under both § 102(e) and § 103(a), Applicants assert that numerous ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

CONCLUSION

Applicants submit the application is in condition for allowance, and an early notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,

/Robert C. Kowert/

Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: June 30, 2011